

日 本 国 特 許 庁
JAPAN PATENT OFFICE

JC879 U.S. PTO
10/053421
01/16/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 9月21日

出 願 番 号

Application Number:

特願2001-288076

出 願 人

Applicant(s):

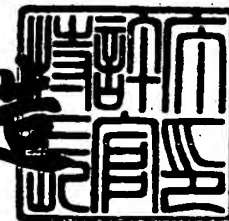
富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年11月26日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3103188

#2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of : Misao KIMURA
Filed: : Concurrently herewith
For: : COMMUNICATION NETWORK SYSTEM...
Serial No. : Concurrently herewith

JC879 U.S. PTO
10/053421
01/16/02

Assistant Commissioner for Patents
Washington, D.C. 20231

January 16, 2002

PRIORITY CLAIM AND SUBMISSION
OF PRIORITY DOCUMENT

S I R:

. Applicant hereby claims priority under 35 USC 119 from JAPANESE patent application no. 2001-288076 filed September 21, 2001, a certified copy of which is enclosed.

Any fee, due as a result of this paper, not covered by an enclosed check, may be charged to Deposit Acct. No. 50-1290.

Respectfully submitted,


Samson Helfgott
Reg. No. 23,072

ROSENMAN & COLIN, LLP
575 MADISON AVENUE
IP Department
NEW YORK, NEW YORK 10022-2584
DOCKET NO.: FUJH 19.343
TELEPHONE: (212) 940-8800

【書類名】 特許願

【整理番号】 0151487

【提出日】 平成13年 9月21日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 12/16
H04L 12/22

【発明の名称】 秘匿機能を有する通信ネットワーク・システムおよび通信方法

【請求項の数】 5

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 木村 操

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100094514

【弁理士】

【氏名又は名称】 林 恒▲徳▼

【代理人】

【識別番号】 100094525

【弁理士】

【氏名又は名称】 土井 健二

【手数料の表示】

【予納台帳番号】 030708

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704944

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 秘匿機能を有する通信ネットワーク・システムおよび通信方法

【特許請求の範囲】

【請求項 1】 中央管理装置と複数の構内ネットワーク・システムとが相互接続され、前記複数の構内ネットワーク・システムのそれぞれは、ルータと端末とが構内ネットワークを介して接続されている通信ネットワーク・システムであって、

前記中央管理装置は、

少なくとも 1 つの共通鍵、ならびに、各ルータおよび該中央管理装置にそれぞれ割り当てられた公開鍵を記憶する管理データベースと、

前記管理データベースに記憶された共通鍵を各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して、各ルータに送信する中央側暗号部と、

を備え、

前記ルータは、

前記中央側暗号部により送信された、暗号化された前記共通鍵を自己の秘密鍵により復号化する第 1 のルータ側復号部と、

前記第 1 のルータ側復号部により復号化された前記共通鍵を記憶する記憶部と

、
自己の構内ネットワーク・システムに設けられた第 1 の送信元端末から他の構内ネットワーク・システムに設けられた第 1 の送信先端末へ送信される通信データ、または、自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して、前記他の構内ネットワークまたは前記中央管理装置に向けて送信するルータ側暗号部と、

を備えている通信ネットワーク・システム。

【請求項 2】 中央管理装置と複数の構内ネットワーク・システムとが相互接続され、前記複数の構内ネットワーク・システムのそれぞれは、ルータと端末とが構内ネットワークを介して接続されている通信ネットワーク・システムにおける通信方法であって、

前記中央管理装置は、管理データベースにあらかじめ記憶された少なくとも1つの共通鍵を、管理データベースにあらかじめ記憶された、各ルータにそれぞれ割り当てられた公開鍵により暗号化して、各ルータに送信し、

前記ルータは、

前記中央管理装置から送信された、暗号化された前記共通鍵を自己の秘密鍵により復号化し、

自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ、または、自己から前記中央管理装置に送信される通信データを前記共通鍵により暗号化して、前記他の構内ネットワークまたは前記中央管理装置に向けて送信する、

通信方法。

【請求項3】 中央管理装置と相互接続された複数の構内ネットワーク・システムのそれぞれに設けられ、該構内ネットワーク・システムのそれぞれに設けられた端末と構内ネットワークを介して接続されたルータであって、

前記中央管理装置から送信された、該ルータの公開鍵により暗号化された共通鍵を自己の秘密鍵で復号化する復号部と、

前記復号部の復号化により得られた共通鍵を記憶する記憶部と、

自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ、または、自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して、前記他の構内ネットワークまたは前記中央管理装置に向けて送信する暗号部と、

を備えているルータ。

【請求項4】 中央管理装置と相互接続された複数の構内ネットワーク・システムのそれぞれに設けられ、該構内ネットワーク・システムのそれぞれに設けられた端末と構内ネットワークを介して接続されたルータの通信方法であって、

前記中央管理装置から送信された、該ルータの公開鍵により暗号化された共通鍵を自己の秘密鍵により復号化して自己の記憶部に記憶し、

自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネッ

トワーク・システムに設けられた送信先端末へ送信される通信データ、または、自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して、前記他の構内ネットワークまたは前記中央管理装置に向けて送信する、

通信方法。

【請求項 5】 ルータと端末とが構内ネットワークを介して接続された複数の構内ネットワーク・システムと相互接続された中央管理装置であって、

ある構内ネットワーク・システムの端末と他の構内ネットワーク・システムの端末との間、または、あるルータと中央管理装置との間で通信されるデータのルータによる暗号化に使用される少なくとも 1 つの共通鍵、ならびに、各ルータおよび該中央管理装置にそれぞれ割り当てられた公開鍵を記憶する管理データベースと、

前記管理データベースに記憶された共通鍵を各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して、各ルータに送信する暗号部と、

を備えている中央管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信データを秘匿する機能を有する通信ネットワーク・システムおよび通信方法に関し、特に、相互接続された複数の構内ネットワーク間で通信されるデータが秘匿される通信ネットワーク・システムおよび通信方法に関する。

【0002】

また、本発明は、通信データを秘匿する機能を有するルータに関する。さらに、本発明は、通信のデータの秘匿に必要な情報の一元管理を行う中央管理装置に関する。

【0003】

【従来の技術】

企業等では、1 つの建物（ビル、工場等）内にイーサネット・ケーブル等の通信ケーブル（たとえば 10BASE-T 等）を張り巡らし、このケーブルにその建物内の

端末（クライアント）やサーバ等を接続して構内ネットワーク（LAN）ないしはイントラネットを構築することが盛んに行われている。

【0004】

また、1つの企業等であっても、たとえばその本社、支社、工場等がそれぞれ異なる場所の異なる建物内に存在する場合には、各建物に構築された構内ネットワークをさらに他の通信回線により相互接続して企業内ネットワークを構築している。この各構内ネットワークを相互接続する通信回線として、一般に、通信事業者が提供する専用線（たとえば通信事業者が提供する公衆ネットワークの一部）が用いられる。

【0005】

このような企業内ネットワークは、インターネットのような開放的で公的なネットワークと異なり、企業等の私的なネットワークであることから、プライベート・ネットワークと呼ばれることがある。

【0006】

このようなプライベート・ネットワークでは、外部の者に対して秘密の情報、すなわち社外秘の情報（たとえば機密情報、社内情報等）が通信されることがある。このような秘密の情報は、当然のことながら、外部の者による閲覧、複写、改竄等が禁止される。

【0007】

しかしながら、プライベート・ネットワークの一部を構成する専用線は、建物間を接続するものであるので、建物の外部に敷設される。したがって、このような専用線の部分では、建物内部に敷設された構内ネットワークの部分よりも、外部の者（たとえば不正な第三者）による盗聴、改竄等が行われやすくなっている。

【0008】

このため、このような盗聴、改竄等から秘密の情報を守るために、種々の暗号化技術が開発され、プライベート・ネットワークにも提供されている。

【0009】

【発明が解決しようとする課題】

しかし、従来の暗号化の機能は、プライベート・ネットワークの端末（クライアント）に搭載されたメーラやブラウザ等のソフトウェアに組み込まれている。そして、暗号化を行うかどうかは、それを使用するユーザの意識に委ねられている。したがって、各ユーザが情報の秘匿に対して高い意識を持っていなければ、情報の暗号化は行われていないのが実情である。

【 0 0 1 0 】

また、情報の重要度、特に秘匿の対象となる情報であるかどうかは、各ユーザによって異なり、たとえば受信者や第三者にとっては秘匿の対象となる情報であっても、発信者がそのように意識していなければ、暗号化が行われずに送信される。

【 0 0 1 1 】

さらに、プライベート・ネットワークは、建物の外部に敷設された通信回線（たとえば専用線）を使用している部分があるにも関わらず、ユーザは、企業内に閉じたネットワーク（クローズド・ネットワーク）として意識していることが多い。このため、ユーザは、第三者による盗聴、改竄等が行われる危険性を十分に認識していないことが多い。

【 0 0 1 2 】

このような背景から、プライベート・ネットワークにおける情報の暗号化を各個人に委ねるのではなく、システム的にサポートする必要性が高まっている。

【 0 0 1 3 】

また、暗号化を行うときに必要となる暗号鍵／復号鍵を各ユーザが管理するのは煩雑である。たとえば、公開鍵暗号方式では、送信者が送信先（受信者）ごとに異なる公開鍵を管理することが必要となる。また、ネットワークに新たな端末、サーバ、構内ネットワーク等が増設される等のようにシステムが拡張された場合には、これらの増設された端末等の公開鍵を送信者側は新たに管理することが必要となる。このように、送信者側に煩雑な鍵の管理が求められる。

【 0 0 1 4 】

本発明は、このような背景に鑑みなされたものであり、その目的は、複数の構内ネットワーク・システムが相互節則された通信ネットワーク・システムにおい

て、構内ネットワーク間で通信されるデータの秘匿を図ることにある。

【0015】

また、本発明の目的は、通信データの秘匿に必要な情報の一元的な管理を行うことにある。

【0016】

【課題を解決するための手段】

前記目的を達成するために、本発明の第1の側面による通信ネットワーク・システムは、中央管理装置と複数の構内ネットワーク・システムとが相互接続され、前記複数の構内ネットワーク・システムのそれぞれは、ルータと端末とが構内ネットワークを介して接続されている通信ネットワーク・システムであって、前記中央管理装置は、少なくとも1つの共通鍵、ならびに、各ルータおよび該中央管理装置にそれぞれ割り当てられた公開鍵を記憶する管理データベースと、前記管理データベースに記憶された共通鍵を各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して、各ルータに送信する中央側暗号部と、を備え、前記ルータは、前記中央側暗号部により送信された、暗号化された前記共通鍵を自己の秘密鍵により復号化する第1のルータ側復号部と、前記第1のルータ側復号部により復号化された前記共通鍵を記憶する記憶部と、自己の構内ネットワーク・システムに設けられた第1の送信元端末から他の構内ネットワーク・システムに設けられた第1の送信先端末へ送信される通信データ、または、自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して、前記他の構内ネットワークまたは前記中央管理装置に向けて送信するルータ側暗号部と、を備えている。

【0017】

本発明の第1の側面による通信方法は、中央管理装置と複数の構内ネットワーク・システムとが相互接続され、前記複数の構内ネットワーク・システムのそれぞれは、ルータと端末とが構内ネットワークを介して接続されている通信ネットワーク・システムにおける通信方法であって、前記中央管理装置は、管理データベースにあらかじめ記憶された少なくとも1つの共通鍵を、管理データベースにあらかじめ記憶された、各ルータにそれぞれ割り当てられた公開鍵により暗号化

して、各ルータに送信し、前記ルータは、前記中央管理装置から送信された、暗号化された前記共通鍵を自己の秘密鍵により復号化し、自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ、または、自己から前記中央管理装置に送信される通信データを前記共通鍵により暗号化して、前記他の構内ネットワークまたは前記中央管理装置に向けて送信するものである。

【 0 0 1 8 】

本発明の第 1 の側面によると、構内ネットワーク・システム間に亘って通信されるデータは、ルータにより暗号化される。したがって、構内ネットワーク・システムの端末のユーザがデータの秘匿（暗号化）を意識しなくても、構内ネットワーク・システム間に亘って通信されるデータを秘匿することができる。これにより、構内ネットワーク・システム間を接続する通信回線におけるデータの秘匿が行われ、該通信回線における第三者による盗聴、複写、改竄等が防止される。

【 0 0 1 9 】

また、暗号化に使用される共通鍵は、中央管理装置の管理データベースに記憶されたものが各ルータに送信され、各ルータにより使用される。したがって、中央管理装置による共通鍵の一元管理が可能となる。

【 0 0 2 0 】

本発明の第 2 の側面によるルータは、中央管理装置と相互接続された複数の構内ネットワーク・システムのそれぞれに設けられ、該構内ネットワーク・システムのそれぞれに設けられた端末と構内ネットワークを介して接続されたルータであって、前記中央管理装置から送信された、該ルータの公開鍵により暗号化された共通鍵を自己の秘密鍵で復号化する復号部と、前記復号部の復号化により得られた共通鍵を記憶する記憶部と、自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ、または、自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して、前記他の構内ネットワークまたは前記中央管理装置に向けて送信する暗号部と、を備えている。

【 0 0 2 1 】

本発明の第2の側面による通信方法は、中央管理装置と相互接続された複数の構内ネットワーク・システムのそれぞれに設けられ、該構内ネットワーク・システムのそれぞれに設けられた端末と構内ネットワークを介して接続されたルータの通信方法であって、前記中央管理装置から送信された、該ルータの公開鍵により暗号化された共通鍵を自己の秘密鍵により復号化して自己の記憶部に記憶し、自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ、または、自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して、前記他の構内ネットワークまたは前記中央管理装置に向けて送信するものである。

【 0 0 2 2 】

本発明の第2の側面によっても、前記第1の側面と同様の作用効果を得ることができる。

【 0 0 2 3 】

本発明の第3の側面による中央管理装置は、ルータと端末とが構内ネットワークを介して接続された複数の構内ネットワーク・システムと相互接続された中央管理装置であって、ある構内ネットワーク・システムの端末と他の構内ネットワーク・システムの端末との間、または、あるルータと中央管理装置との間で通信されるデータのルータによる暗号化に使用される少なくとも1つの共通鍵、ならびに、各ルータおよび該中央管理装置にそれぞれ割り当てられた公開鍵を記憶する管理データベースと、前記管理データベースに記憶された共通鍵を各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して、各ルータに送信する暗号部と、を備えている。

【 0 0 2 4 】

本発明の第3の側面によると、構内ネットワーク・システム間で通信されるデータの暗号化に使用される共通鍵を中央管理装置によって一元管理することができる。

【 0 0 2 5 】

【発明の実施の形態】

以下に、本発明の実施の形態について説明するが、これは例であって、本発明の技術的範囲を限定するものではない。

【 0 0 2 6 】

図 1 は、本発明の実施の形態による通信ネットワーク・システム 10 の全体構成を示すブロック図である。この通信ネットワーク・システム 10 は、ある企業（企業 A とする。）のプライベート・ネットワーク・システムであり、専用線ネットワーク 1、中央管理装置 2、および複数（ n 個： n は 2 以上の整数）の構内ネットワーク・システム $3_1 \sim 3_n$ を備えている。

【 0 0 2 7 】

専用線ネットワーク 1 は、通信事業者が提供する専用線により構成された通信ネットワークである。この専用線には、公衆ネットワークの一部が割り当てられることもある。

【 0 0 2 8 】

各構内ネットワーク・システム $3_1 \sim 3_n$ は、たとえば、企業 A の本社、工場、営業所等の構内にそれぞれ設置されているイントラネットである。各構内ネットワーク・システム $3_1 \sim 3_n$ は、構内ネットワークないしは私設ネットワーク（たとえばイーサネット等の LAN） $4_1 \sim 4_n$ 、ルータ $5_1 \sim 5_n$ 、および、1 または 2 以上の端末 $6_{11} \sim 6_{1p} \dots 6_{n1} \sim 6_{nq}$ （ p および q は 1 以上の整数）を備えている。

【 0 0 2 9 】

以下では、各構内ネットワーク・システム $3_1 \sim 3_n$ を、これらを特に区別して用いる場合を除き、「構内ネットワーク・システム 3」と総称する。同様にして、特に区別して用いる場合を除き、私設ネットワーク $4_1 \sim 4_n$ を「構内ネットワーク 4」と総称し、ルータ $5_1 \sim 5_n$ を「ルータ 5」と総称し、端末 $6_{11} \sim 6_{1p} \dots 6_{n1} \sim 6_{nq}$ を「端末 6」と総称する。

【 0 0 3 0 】

各ルータ 5 および中央管理装置 2 は、専用線ネットワーク 1 に接続され、専用線ネットワーク 1 を介して相互に通信可能に構成されている。また、各構内ネットワーク・システム 3 に設けられたルータ 5 および端末 6 は、構内ネットワーク

4に接続され、相互に通信可能に構成されている。専用線ネットワーク1および構内ネットワーク4を介して通信されるデータ（メッセージ）は、本実施の形態では、IPパケットにより搬送される。端末6は、たとえば企業Aの経営者、従業員等が使用するパソコン、ワークステーション等であり、クライアントと呼ばれることもある。

【0031】

ルータ5の代わりに、ファイアウォールが専用線ネットワーク1に接続されることがある。この場合には、ルータ5は、ファイアウォールに接続され、ファイアウォールを介して専用線ネットワーク1に接続されることとなる。

【0032】

中央管理装置2も、ルータ5と同様に、ある企業の構内に配置されており、構内ネットワーク・システム（構内ネットワーク・システム $3_1 \sim 3_n$ のいずれかまたは異なる構内ネットワーク・システム）に設けられていてもよい。中央管理装置2は、ルータまたはファイアウォールにより構成することができる。

【0033】

中央管理装置2には、後に詳述する管理データベース20が設けられている。管理データベース20は、後に詳述するように、各端末6間で通信されるデータ（IPパケット）の暗号化の必要の有無に関する情報と、暗号化のための鍵に関する情報とを有し、これらの情報を通信ネットワーク・システム10において一元管理する。管理データベース20に設けられた情報の一部は、各ルータ5に与えられ、端末6間で通信されるデータの暗号化／復号化の際に使用される。

【0034】

ある構内ネットワーク・システム3内の端末6（送信元端末）が他の構内ネットワーク・システム3内の端末6（送信先端末）にデータを送信する場合に、このデータは、送信元端末の構内ネットワーク・システム3に設けられたルータ5（送信元ルータ）を経由して専用線ネットワーク1に送信され、専用線ネットワーク1から送信先端末のある構内ネットワーク・システム3のルータ5（送信先ルータ）を経由する。

【0035】

この際、本実施の形態では、送信元ルータが、送信されるデータを暗号化する必要があるかどうかを判断する。この判断は、管理データベース 20 から与えられた情報に基づいて行われる。暗号化の必要がある場合に、送信元ルータはデータを暗号化し、送信先ルータに送信する。

【0036】

一方、送信先ルータは、送信元ルータから送信されたデータを復号化の必要があるかどうかを判断する。この判断も、管理データベース 20 から与えられた情報に基づいて行われる。復号化の必要がある場合に、送信先ルータは、データを復号化し、同じ構内ネットワーク・システムに設けられた送信先端末に、復号化されたデータを送信する。

【0037】

このように、本実施の形態では、異なる構内ネットワーク・システム 3 間に亘って通信されるメッセージに対して、ルータ 5 による暗号化および復号化が行われる。これにより、構内ネットワーク・システム 3 間に亘って通信されるデータの第三者による盗聴、複写、改竄等が有効に防止される。また、ルータがデータの暗号化／復号化の必要性を判断し、必要な場合には暗号化／復号化を行うので、情報の秘匿を確実に行うことができる。

【0038】

なお、同一の構内ネットワーク・システム 3 内で通信されるメッセージに対しては、従来のシステムと同様にして、各端末 6 のメーラまたはブラウザに設けられた暗号化機能により、暗号化および復号化が行われることとなる。

【0039】

以下、管理データベース 20 が有する情報の詳細、ルータ 5 の詳細な構成、および暗号化／復号化の処理の詳細について説明する。

【0040】

図 2 ～ 図 4 は、管理データベース 20 が有するデータを示している。管理データベース 20 は、秘匿端末テーブル（図 2）、公開鍵／秘密鍵テーブル（図 3（A）または（B））、および共通鍵テーブル（図 4（A）および（B））のデータを有する。これらのデータは、通信ネットワーク・システム 10 の管理者、中

央管理装置 2 のオペレータ等が中央管理装置 2 を操作して入力される。

【 0 0 4 1 】

図 2 を参照して、秘匿端末テーブルは、ルータの欄、加入端末の欄、および相手先端末の欄を有し、端末 6 間で通信されるデータのうち、秘匿（すなわち暗号化（および復号化））の必要があるデータが送受信される 2 つの端末（すなわち図 2 における加入端末および相手先端末）の組み合わせを示している。すなわち、この秘匿端末テーブルに示される加入端末と相手先端末との間でデータが通信される場合に、そのデータは暗号化／復号化されることとなる。

【 0 0 4 2 】

ルータの欄は、通信ネットワーク・システム 1 0 において各ルータ 5 を識別するための識別情報を有する。この識別情報として、たとえばルータ 5 の IP アドレスが使用される。ただし、この識別情報は通信ネットワーク・システム 1 0 において各ルータ 5 を識別できる情報であればよいので、IP アドレスの一部や、各ルータ 5 の名称等がこの識別情報として使用されてもよい。

【 0 0 4 3 】

加入端末の欄は、ルータの欄に設けられたルータ 5 に加入している（すなわちルータ 5 に構内ネットワーク 4 を介して直接接続されている）端末 6 の識別情報を有する。たとえば端末 6_{11} 、 6_{12} 、 6_{1p} 等は、ルータ 5_1 に加入しており、該ルータ 5_1 に構内ネットワーク 4_1 を介して直接接続されている。

【 0 0 4 4 】

相手先端末の欄は、加入端末の欄に設けられた端末 6 とデータを通信する際に、秘匿の必要がある通信相手の端末の識別情報を有する。たとえば、加入端末 6_{11} と、これに対応する相手先端末 6_{21} または 6_{25} との間で通信されるデータは秘匿（すなわち暗号化（および復号化））の必要がある。

【 0 0 4 5 】

加入端末が送信元端末となり、相手先端末が送信先端末となる場合もあるし、その逆の場合もある。いずれの場合も、通信されるデータは、秘匿される。

【 0 0 4 6 】

加入端末および相手先端末の欄に格納される識別情報として、たとえば端末 6

のIPアドレスが使用される。ただし、ルータの欄と同様に、この識別情報は、通信ネットワーク・システム10において各端末6を識別できる情報であればよいので、IPアドレスの一部、各端末6の名称等が使用されてもよい。

【0047】

なお、秘匿端末テーブルは、秘匿が必要なデータと秘匿が必要でないデータとを分別するために使用されるので、すべての端末6間で通信されるデータに対して秘匿が必要とされる場合には、この秘匿端末テーブルを管理データベース20に設ける必要はない。

【0048】

図3(A)を参照して、公開鍵／秘密鍵テーブルは、中央管理装置2の公開鍵および秘密鍵の組み合わせ、ならびに、各ルータ5の公開鍵および秘密鍵の組み合わせを示すデータである。

【0049】

ルータの欄には、データおよびこのデータを暗号化するために使用された共通鍵の送信先となるルータ（ルータ5または中央管理装置2）の識別情報が設けられる。公開鍵の欄には、ルータの欄に設けられた送信先ルータに送信されるデータを暗号化および復号化するための共通鍵を暗号化するための公開鍵が設けられる。秘密鍵の欄には、送信先ルータが該共通鍵を復号化するための共通鍵が設けられる。

【0050】

たとえば、あるルータ5から中央管理装置2へ送信されるデータを暗号化するために使用された共通鍵は、中央管理装置2の公開鍵 K_{pc} により暗号化され、中央管理装置2に送信される。中央管理装置2は、暗号化された共通鍵を秘密鍵 K_{sc} により復号化する。同様にして、ルータ 5_1 以外のルータ5または中央管理装置2からルータ 5_1 に送信されるデータを暗号化するために使用された共通鍵は、ルータ 5_1 の公開鍵 K_{p1} により暗号化され、ルータ 5_1 に送信される。ルータ 5_1 は、暗号化された共通鍵を秘密鍵 K_{s1} により復号化する。他のルータの公開鍵および秘密鍵についても同様である。

【0051】

公開鍵／秘密鍵の組み合わせを、図 3 (B) に示すように、相手ルータ（すなわち送信元ルータ（ルータ 5 または中央管理装置 2））ごとに個別に設けることもできる。たとえば、ルータ 5₁ が中央管理装置 2 にデータを送信する場合に、ルータ 5₁ は相手ルータ 5₁ に対応する公開鍵 K_{pc1} により共通鍵を暗号化し、中央管理装置 2 は相手ルータ 5₁ に対応する秘密鍵 K_{sc1} により共通鍵を復号化する。他のルータの公開鍵および秘密鍵についても同様である。

【 0 0 5 2 】

図 4 (A) を参照して、共通鍵テーブルは、複数の共通鍵から構成される。各ルータ 5 および中央管理装置 2 は、この複数の共通鍵の中から任意の 1 つを選択して、メッセージを暗号化する。選択の方法は、各ルータ 5 および中央管理装置 2 に委ねられる。

【 0 0 5 3 】

図 4 (B) に示すように、共通鍵テーブルには、共通鍵の欄に加えて、各共通鍵に対応した共通鍵暗号方法（共通鍵暗号方式）を設けることができる。たとえば、共通鍵 K_{c1} には暗号方法 M₁ が、共通鍵 K_{c2} には暗号方法 M₂ が、それぞれ使用される。各共通鍵に対応する暗号化方法は、他の共通鍵に対応する暗号方法と同じものであってもよいし、異なるものであってもよい。共通鍵暗号方法には、DES (Data Encryption Standard)、AES (Advanced Encryption Standard) 等がある。

【 0 0 5 4 】

管理データベース 20 に格納されたこれらのデータ（テーブル）の一部は、中央管理装置 2 から専用線ネットワーク 1 を介して各ルータ 5 に送信され、各ルータ 5 の内部メモリ（半導体メモリ、ハードディスク等）に記憶される。この送信は、送信するデータを、管理データベース 20 に記憶された共通鍵（図 4 (A) または (B) 参照）の 1 つにより暗号化するとともに、該共通鍵を、送信先となるルータ 5 の公開鍵により暗号化して、送信するデータに付加して行われる。受信側のルータ 5 は、暗号化された共通鍵を自己の秘密鍵により復号化し、この復号化された共通鍵により、暗号化されたデータを復号化する。これらの送受信の処理は、後述する図 8 および図 9 のフローチャートに示すものと同様である。

【0055】

図5は、ルータ5のうちルータ5₁を例にとり、該ルータ5₁が有するデータを示している。同図(A)は秘匿端末テーブルを、同図(B)は公開鍵／秘密鍵テーブルを、同図(C)は共通鍵テーブルを、それぞれ示している。

【0056】

図5(A)を参照して、参照ルータ5₁が有する秘匿端末テーブルは、管理データベース20が有する秘匿端末テーブル(図2参照)のうち、ルータの欄がルータ5₁に関する部分のみを有する。すなわち、ルータ5₁が有する秘匿端末テーブルは、ルータ5₁の加入端末とその相手先端末との対応表の部分のみを有する。

【0057】

図5(B)を参照して、ルータ5₁が有する公開鍵／秘密鍵テーブルは、管理データベース20が有する公開鍵／秘密鍵テーブル(図3(A)参照)のうち、自身(すなわちルータ5₁)の公開鍵および秘密鍵、ならびに他のルータ5および中央管理装置2の公開鍵のみを有する。公開鍵／秘密鍵テーブルが図3(B)に示すものである場合には、ルータ5₁が有する公開鍵／秘密鍵テーブルも、同様に、相手ルータごとに個別に設けられる。

【0058】

図5(C)を参照して、ルータ5₁が有する共通鍵テーブルは、管理データベース20が有するもの(図4(A)または(B)参照)と同じである。

【0059】

他のルータ5₂～5_nが有するテーブルも、ルータ5₁が有するテーブルと同様である。

【0060】

これらのテーブル以外に、各ルータ5は、ルータであるので、経路制御を行うためのルーティング・テーブル等、一般のルータが備えているデータを有することはいふまでもない。

【0061】

各ルータ5は、このようなテーブルに基づいて、通信データの暗号化および復

号化を行い、暗号化されたデータのルーティングおよび加入端末への配信を行う。図6は、加入端末6（送信元端末）からデータを受信した送信元ルータが送信先ルータの加入端末6（送信先端末）に該データを送信する場合の処理の流れを示すフローチャートである。

【0062】

送信元ルータが、構内ネットワーク4を介して自身に直接接続された送信元端末からデータ（IPパケット）を受信すると（ステップS1でYES）、該送信元ルータは、該メッセージが秘匿（すなわち暗号化）の対象かどうかを判断する（ステップS2）。

【0063】

この判断は、データのヘッダ部に含まれる送信元端末のIPアドレスおよび送信先端末のIPアドレスと、自身に記憶されている秘匿端末テーブル（図5（A）参照）とを比較することにより行われる。送信元端末のIPアドレスおよび送信先端末のIPアドレスの組み合わせが秘匿端末テーブルに存在する場合には、そのデータは秘匿対象であると判断され、存在しない場合には、そのデータは秘匿対象でないと判断される。

【0064】

データが秘匿対象であると判断されると（ステップS2でYES）、送信元ルータは、ルーティング・テーブルに基づいて、送信先ルータを特定し、特定した送信先ルータの公開鍵を、自身に記憶されている公開鍵／秘密鍵テーブル（図5（B）参照）から選択する（ステップS3）。

【0065】

続いて、送信元ルータは、データを暗号化するための共通鍵を、自身に記憶された共通鍵テーブル（図5（C）参照）から選択する（ステップS4）。そして、送信側ルータは、選択した共通鍵を用いてデータ（本実施の形態では、IPパケットのデータ部のみ）を暗号化する（ステップS5）。

【0066】

次に、送信元ルータは、ステップS3で選択された公開鍵を用いて、データ部の暗号に使用された共通鍵を暗号化し（ステップS6）、この暗号化された共通

鍵をIPパケットのデータ部に付加する。暗号化された共通鍵をデータ部のどの箇所に付加するかは、送信元ルータと送信先ルータとの間であらかじめ定められている。たとえば、データ部の先頭、最後尾等の箇所に、暗号化された共通鍵が付加される。

【0067】

次に、送信元ルータは、暗号化された共通鍵をデータ部に付加することに伴って生じる、IPパケットのヘッダ部の変更を行う（ステップS8）。変更を行う箇所として、IPv4の場合には、ヘッダ部のヘッダ長、全長、ID、およびフラグがある。これらの各値が、暗号化された共通鍵を付加した後の値に変更される。

【0068】

続いて、送信元ルータは、このIPパケットを専用線ネットワーク1を介して送信先ルータに送信する（ステップS9）。その後、処理は、ステップS1に戻る。なお、IPパケットが送信元ルータから送信先ルータに届くまでに1または2以上の中継ルータ（ルータ5のいずれか）を経由する場合には、これらの中継ルータは、インターネットにおける一般の中継ルータと同様に、ルーティング・テーブルに基づいて、IPパケットをルーティングする。

【0069】

ステップS2において、データが秘匿対象でないと判断されると（ステップS2でNO）、処理はステップS9に進み、データは暗号化等の処理を受けることなく、そのまま送信元ルータから送信される。

【0070】

なお、すべてのデータが暗号化の対象となる場合には、ステップS2の処理は省略される。

【0071】

図7は、送信先ルータの処理の流れを示すフローチャートである。送信先ルータは、送信元ルータからデータ（IPパケット）を受信すると（ステップS11）、受信したデータが秘匿対象であるかどうかを判断する（ステップS12）。この判断は、前述したステップS2の判断と同様に、IPパケットのヘッダ部に

含まれる発信元アドレス（IPアドレス）および宛先アドレス（IPアドレス）と、自己に記憶された秘匿対象テーブル（図5（A）参照）とを比較することにより行われる。

【0072】

データが秘匿対象であると判断された場合には（ステップS12でYES）、送信先ルータは、自己に記憶された公開鍵／秘密鍵テーブル（図5（B）参照）から、自己の秘密鍵を選択する（ステップS13）。

【0073】

次に、送信先ルータは、暗号化された共通鍵を、データ（IPパケット）のデータ部から抽出する（ステップS14）。前述したように、暗号化された共通鍵が付加された箇所はルータ間であらかじめ定められているので、送信先ルータは、このあらかじめ定められた箇所から共通鍵を抽出する。

【0074】

続いて、送信先ルータは、抽出された共通鍵を、ステップS13で選択された秘密鍵により復号化する（ステップS15）。そして、送信先ルータは、復号化により得られた共通鍵により、データ部を復号化する（ステップS16）。図4（B）に示すように、共通鍵に対応して暗号化方法が定められている場合には、送信先ルータは、自己に記憶された共通鍵テーブルから、復号化された共通鍵に対応する暗号化方法を選択し、この共通鍵および選択された暗号化方法に基づいて、データ部を復号化する。

【0075】

続いて、送信先ルータは、データ部の復号化およびデータ部からの共通鍵の抽出に伴い生じるIPパケットのヘッダ部の変更（すなわち暗号化前の状態に復元）を行う（ステップS17）。

【0076】

その後、送信先ルータは、復元されたIPパケットを、自己に直接接続された送信先端末（加入端末）に構内ネットワーク4を介して送信する（ステップS18）。その後、処理は、ステップS11に戻る。

【0077】

ステップS12において、データが秘匿対称でないと判断されると（ステップS2でNO）、処理はステップS18に進み、データは復号化等の処理を受けることなく、そのまま端末に送信される。

【0078】

なお、すべてのデータが復号化の対象となる場合には、ステップS12の処理は省略される。

【0079】

このように、本実施の形態では、ルータ5が、あらかじめ定められた秘匿端末テーブルに基づいてデータを暗号化／復号化するので、端末6のユーザが特に秘匿を意識しなくても、情報（たとえば社外秘の情報等）を第三者の盗聴、複写、改竄等から有効に守ることができる。

【0080】

次に、管理データベース20に記憶されたテーブルが更新された場合の各ルータに記憶されたテーブルの更新処理について説明する。

【0081】

通信ネットワーク・システム10の暗号化／復号化に必要な情報は、中央管理装置2および管理データベース20によって一元管理されるので、この情報に変更が生じると、まず管理データベース20の情報が更新される。

【0082】

この管理データベース20の更新は、ある構内ネットワーク・システム3に新たな端末6が追加された場合、ある構内ネットワーク・システム3から既設の端末6が取り除かれた場合、新たな構内ネットワーク・システム3が通信ネットワーク・システム10に追加された場合、既設の構内ネットワーク・システム3が通信ネットワーク・システム10から取り除かれた場合、公開鍵、秘密鍵、または共通鍵に追加、変更、または削除が生じた場合等に行われる。

【0083】

たとえば、ある構内ネットワーク・システム3に新たな端末6が追加された場合に、新たに追加された端末に関する情報が秘匿対象テーブル（図2参照）に追加される。また、新たな構内ネットワーク・システム3が追加された場合には、

秘匿対象テーブルには、新たに追加された構内ネットワーク・システム 3 のルータ 5 および端末 6 に関する情報が追加され、公開鍵／秘密鍵テーブル（図 3（A）または（B）参照）には、新たに追加された構内ネットワーク・システム 3 のルータ 5 に関する情報（公開鍵および秘密鍵）が追加される。公開鍵または秘密鍵に変更が生じた場合には、公開鍵／秘密鍵テーブルが変更され、共通鍵（または暗号化方法）に変更が生じた場合には、共通鍵テーブル（図 4（A）または（B）参照）が変更される。

【 0 0 8 4 】

また、これらの場合に加えて、管理データベース 2 0 は、同一の状態が長期間継続することを避け、セキュリティを高めるために、定期的に更新されることが好ましい。

【 0 0 8 5 】

この管理データベース 2 0 の更新は、通信ネットワーク・システム 1 0 の管理者、中央管理装置 2 のオペレータ等が中央管理装置 2 を操作することにより行われる。

【 0 0 8 6 】

管理データベース 2 0 が更新されると、管理データベース 2 0 の更新を各ルータ 5 に記憶されたテーブルにも反映させるために、更新された部分が更新の必要なルータ 5 に送信される。図 8 は、管理データベース 2 0 の秘匿対象テーブル、公開鍵／秘密鍵テーブル、または共通鍵テーブルが更新された場合における中央管理装置 2 の処理の流れを示すフローチャートである。

【 0 0 8 7 】

まず、中央管理装置 2 は、更新されたテーブルを送信する対象となるルータ（送信先ルータ）のテーブルを作成する（ステップ S 2 1）。

【 0 0 8 8 】

続いて、中央管理装置 2 は、送信先ルータの公開鍵を公開鍵／秘密鍵テーブルから選択する（ステップ S 2 2）。ここで、公開鍵／秘密鍵テーブルが更新されている場合には、公開鍵が選択される公開鍵／秘密鍵テーブルは更新前のものである（すなわち、選択される公開鍵も更新前のものである）ことが好ましい。こ

れは、更新された公開鍵／秘密鍵テーブルを受信する送信先ルータは、更新された公開鍵／秘密鍵を受信し、自己のデータの更新が完了するまでは、更新前の秘密鍵を用いて復号化を行うからである。したがって、管理データベース 2 0 には、各ルータに記憶されたデータの更新が完了するまでは、更新前のデータも一時的に保持されることが好ましい。

【 0 0 8 9 】

続いて、中央管理装置 2 は、送信先ルータの共通鍵を共通鍵テーブルから選択する（ステップ S 2 3）。ここで、前述した公開鍵／秘密鍵テーブルと同様に、共通鍵テーブルについても、更新されている場合には、共通鍵が選択される共通鍵テーブルは更新前のものである（すなわち、選択される共通鍵も更新前のものである）ことが好ましい。

【 0 0 9 0 】

次に、中央管理装置 2 は、ステップ S 2 3 で選択された共通鍵により、ステップ S 2 1 において準備されたテーブルから作成された I P パケットのデータ部を暗号化する（ステップ S 2 4）。準備されたテーブルが複数の I P パケットに分割される場合には、各 I P パケットのデータ部が共通鍵により暗号化される。

【 0 0 9 1 】

続いて、中央管理装置 2 は、ステップ S 2 2 で選択された公開鍵により、共通鍵を暗号化する（ステップ S 2 5）。

【 0 0 9 2 】

続いて、前述した図 6 のステップ S 7 の処理と同様に、中央管理装置 2 は、暗号化された共通鍵を I P パケットのデータ部に付加する（ステップ S 2 6）。これに伴い、付加された I P パケットのヘッダ部が変更される。テーブルが複数の I P パケットに分割されて送信される場合に、暗号化された共通鍵は、先頭の I P パケットに付加されることが好ましい。

【 0 0 9 3 】

続いて、中央管理装置 2 は、これらの暗号化されたテーブルおよび共通鍵を送信先ルータに送信する（ステップ S 2 7）。

【 0 0 9 4 】

一方、送信先ルータは、更新されたテーブルが送信されると、このテーブルにより、自己に記憶されたデータを更新する。図9は、更新されたテーブルが中央管理装置2から送信された場合における送信先ルータの処理の流れを示すフローチャートである。

【0095】

送信先ルータは、暗号化されたテーブルおよび共通鍵を中央管理装置2から受信すると（ステップS31）、秘密鍵を選択し（ステップS32）、暗号化された共通鍵を選択した秘密鍵により復号化する（ステップS33）。ここで、中央管理装置2から送信されたテーブルが公開鍵／秘密鍵テーブルであり、公開鍵／秘密鍵テーブルを更新する場合であっても、ステップS32で選択される秘密鍵は、送信先ルータに既に記憶されているもの（すなわち更新前のもの）である。

【0096】

続いて、送信先ルータは、共通鍵でテーブルを復号化する（ステップS34）。テーブルが複数のIPパケットに分割され、送信されている場合には、各IPパケットのデータ部が復号化され、復号化された複数のデータ部を結合することにより、テーブルが再構築されることとなる。

【0097】

続いて、送信先ルータは、復号化されたテーブルにより、自己に記憶されたテーブルを置換（更新）する（ステップS35）。これにより、送信先ルータのテーブルの更新が終了する。

【0098】

このように、本実施の形態では、秘匿端末テーブル、公開鍵／秘密鍵テーブル、および共通鍵テーブルが中央管理装置2および管理データベース20によって一元管理される。そして、更新された場合には、更新された情報が、中央管理装置2から各ルータ5に送信され、ルータ5の保持するデータが更新される。したがって、端末6のユーザが鍵を管理したり、データの暗号化／復号化の必要の有無を判断したりする煩雑さが解消される。また、通信ネットワーク・システム10に変更が生じたい場合にも、この変更に対応することができる。

【0099】

これまで述べた実施の形態では、IP パケット単位で暗号化を行っているが、送信対象となるデータ全体を先に暗号化し、暗号化されたデータ全体を IP パケットに分割して送信することもできる。また、送信元ルータによって使用される共通鍵が送信先ルータにあらかじめ判明している場合には、この共通鍵は、公開鍵により暗号化されて送信先ルータに送信されなくてもよい。

【0100】

なお、図6から図9に示す各フローチャートの処理は、ルータ5または中央管理装置2に組み込まれるプログラムにより記述することもできるし、ハードウェア回路により実現することもできる。

【0101】

(付記1) 中央管理装置と複数の構内ネットワーク・システムとが相互接続され、前記複数の構内ネットワーク・システムのそれぞれは、ルータと端末とが構内ネットワークを介して接続されている通信ネットワーク・システムであって

前記中央管理装置は、

少なくとも1つの共通鍵、ならびに、各ルータおよび該中央管理装置にそれぞれ割り当てられた公開鍵を記憶する管理データベースと、

前記管理データベースに記憶された共通鍵を各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して、各ルータに送信する中央側暗号部と、

を備え、

前記ルータは、

前記中央側暗号部により送信された、暗号化された前記共通鍵を自己の秘密鍵により復号化する第1のルータ側復号部と、

前記第1のルータ側復号部により復号化された前記共通鍵を記憶する記憶部と

自己の構内ネットワーク・システムに設けられた第1の送信元端末から他の構内ネットワーク・システムに設けられた第1の送信先端末へ送信される通信データ、または、自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して、前記他の構内ネットワークまたは前記

中央管理装置に向けて送信するルータ側暗号部と、
を備えている通信ネットワーク・システム。

【0102】

(付記2) 付記1において、
前記中央側暗号部は、前記公開鍵をさらに暗号化して各ルータに送信し、
前記第1のルータ側復号部は、前記中央側暗号部により暗号化された前記公開鍵を自己の秘密鍵により復号化し、
前記記憶部は、前記復号化された公開鍵を記憶し、
前記ルータ側暗号部は、前記記憶部に記憶された公開鍵から、前記送信先となる他の構内ネットワーク・システムのルータまたは前記中央管理装置の公開鍵を選択し、該選択した公開鍵により前記共通鍵を暗号化し、該暗号化された共通鍵を前記暗号化された通信データとともに前記他の構内ネットワークまたは前記中央管理装置に向けて送信する、
通信ネットワーク・システム。

【0103】

(付記3) 付記1または2において、
前記管理データベースは、前記複数の構内ネットワーク・システムのあるものの端末と他のものの端末との組み合わせのうち、これらの端末間の通信データを暗号化する必要がある組み合わせを示す秘匿端末データをさらに記憶し、
前記中央側暗号部は、前記秘匿端末データを各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して、各ルータに送信し、
前記第1のルータ側復号部は、前記中央側暗号部により送信された、暗号化された前記秘匿端末データを自己の秘密鍵により復号化し、
前記記憶部は、前記復号化された秘匿端末データを記憶し、
前記ルータ側暗号部は、前記第1の送信元端末および前記第1の送信先端末の組み合わせが前記秘匿端末データに含まれている場合には、前記通信データを暗号化し、含まれていない場合には前記通信データを暗号化しない、
通信ネットワーク・システム。

【0104】

(付記 4) 付記 1 または 2 において、

前記ルータは、他の構内ネットワーク・システムに設けられた第 2 の送信元端末から自己の構内ネットワーク・システムに設けられた第 2 の送信先端末に送信されてきたデータを復号化して、該自己の構内ネットワーク・システムに設けられた前記第 2 の送信先端末に送信する第 2 のルータ側復号部をさらに備えている通信ネットワーク・システム。

【 0 1 0 5 】

なお、ここで、第 2 の送信元端末と第 1 の送信先端末とは、同じ端末であってもよいし、異なる端末であってもよい。同様に、第 2 の送信先端末と第 1 の送信元端末とは、同じ端末であってもよいし、異なる端末であってもよい。

【 0 1 0 6 】

(付記 5) 付記 4 において、

前記管理データベースは、前記複数の構内ネットワーク・システムのあるものの端末と他のものの端末との組み合わせのうち、これらの端末間の通信データを暗号化する必要がある組み合わせを示す秘匿端末データをさらに記憶し、

前記中央側暗号部は、前記秘匿端末データを各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して、各ルータに送信し、

前記第 1 のルータ側復号部は、前記中央側暗号部により送信された、暗号化された前記秘匿端末データを自己の秘密鍵により復号化し、

前記記憶部は、前記復号化された秘匿端末データを記憶し、

前記第 2 のルータ側復号部は、前記第 2 の送信元端末および前記第 2 の送信先端末の組み合わせが前記秘匿端末データに含まれている場合には、前記通信データを復号化し、含まれていない場合には前記通信データを復号化しない、

通信ネットワーク・システム。

【 0 1 0 7 】

(付記 6) 付記 1 において、

前記管理データベースに記憶された共通鍵が更新された場合に、前記中央側暗号部は更新された共通鍵を暗号化して送信し、前記第 1 のルータ側復号部は更新された共通鍵を復号化し、前記記憶部はすでに記憶された共通鍵を更新された共

通鍵に置換して記憶する、通信ネットワーク・システム。

【0108】

(付記7) 付記2において、

前記管理データベースに記憶された公開鍵が更新された場合に、前記中央側暗号部は更新された公開鍵を暗号化して送信し、前記第1のルータ側復号部は更新された公開鍵を復号化し、前記記憶部はすでに記憶された公開鍵を更新された公開鍵に置換して記憶する、通信ネットワーク・システム。

【0109】

(付記8) 付記3または5において、

前記管理データベースに記憶された前記秘匿端末データが更新された場合に、前記中央側暗号部は更新された秘匿端末データを暗号化して送信し、前記第1のルータ側復号部は更新された秘匿端末データを復号化し、前記記憶部はすでに記憶された秘匿端末データを更新された秘匿端末データに置換して記憶する、通信ネットワーク・システム。

【0110】

(付記9) 中央管理装置と複数の構内ネットワーク・システムとが相互接続され、前記複数の構内ネットワーク・システムのそれぞれは、ルータと端末とが構内ネットワークを介して接続されている通信ネットワーク・システムにおける通信方法において、

前記中央管理装置は、管理データベースにあらかじめ記憶された少なくとも1つの共通鍵を、管理データベースにあらかじめ記憶された、各ルータにそれぞれ割り当てられた公開鍵により暗号化して、各ルータに送信し、

前記ルータは、

前記中央管理装置から送信された、暗号化された前記共通鍵を自己の秘密鍵により復号化し、

自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ、または、自己から前記中央管理装置に送信される通信データを前記共通鍵により暗号化して、前記他の構内ネットワークまたは前記中央管理装置に向けて送信する、

通信方法。

【 0 1 1 1 】

(付記 1 0) 中央管理装置と相互接続された複数の構内ネットワーク・システムのそれぞれに設けられ、該構内ネットワーク・システムのそれぞれに設けられた端末と構内ネットワークを介して接続されたルータであって、

前記中央管理装置から送信された、該ルータの公開鍵により暗号化された共通鍵を自己の秘密鍵で復号化する復号部と、

前記復号部の復号化により得られた共通鍵を記憶する記憶部と、

自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ、または、自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して、前記他の構内ネットワークまたは前記中央管理装置に向けて送信する暗号部と、

を備えているルータ。

【 0 1 1 2 】

(付記 1 1) 中央管理装置と相互接続された複数の構内ネットワーク・システムのそれぞれに設けられ、該構内ネットワーク・システムのそれぞれに設けられた端末と構内ネットワークを介して接続されたルータの通信方法であって、

前記中央管理装置から送信された、該ルータの公開鍵により暗号化された共通鍵を自己の秘密鍵により復号化して自己の記憶部に記憶し、

自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ、または、自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して、前記他の構内ネットワークまたは前記中央管理装置に向けて送信する、

通信方法。

【 0 1 1 3 】

(付記 1 2) 中央管理装置と相互接続された複数の構内ネットワーク・システムのそれぞれに設けられ、該構内ネットワーク・システムのそれぞれに設けら

れた端末と構内ネットワークを介して接続されたルータに、

前記中央管理装置から送信された、該ルータの公開鍵により暗号化された共通鍵を自己の秘密鍵により復号化して自己の記憶部に記憶する手順と、

自己の構内ネットワーク・システムに設けられた送信元端末から他の構内ネットワーク・システムに設けられた送信先端末へ送信される通信データ、または、自己から前記中央管理装置に送信される通信データを前記記憶部に記憶された前記共通鍵により暗号化して、前記他の構内ネットワークまたは前記中央管理装置に向けて送信する手順と、

を実行させるためのプログラム。

【0114】

(付記13) ルータと端末とが構内ネットワークを介して接続された複数の構内ネットワーク・システムと相互接続された中央管理装置であって、

ある構内ネットワーク・システムの端末と他の構内ネットワーク・システムの端末との間、または、あるルータと中央管理装置との間で通信されるデータのルータによる暗号化に使用される少なくとも1つの共通鍵、ならびに、各ルータおよび該中央管理装置にそれぞれ割り当てられた公開鍵を記憶する管理データベースと、

前記管理データベースに記憶された共通鍵を各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して、各ルータに送信する暗号部と、

を備えている中央管理装置。

【0115】

(付記14) ルータと端末とが構内ネットワークを介して接続された複数の構内ネットワーク・システムと相互接続された中央管理装置の管理方法であって

ある構内ネットワーク・システムの端末と他の構内ネットワーク・システムの端末との間、または、あるルータと中央管理装置との間で通信されるデータのルータによる暗号化に使用される少なくとも1つの共通鍵、ならびに、各ルータおよび該中央管理装置にそれぞれ割り当てられた公開鍵を管理データベースに記憶して管理し、

前記管理データベースに記憶された共通鍵を各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して、各ルータに送信する、

管理方法。

【0116】

(付記15) ルータと端末とが構内ネットワークを介して接続された複数の構内ネットワーク・システムと相互接続された中央管理装置に設けられたコンピュータに、

ある構内ネットワーク・システムの端末と他の構内ネットワーク・システムの端末との間、または、あるルータと中央管理装置との間で通信されるデータのルータによる暗号化に使用される少なくとも1つの共通鍵、ならびに、各ルータおよび該中央管理装置にそれぞれ割り当てられた公開鍵を管理データベースに記憶して管理させる手順と、

前記管理データベースに記憶された共通鍵を各ルータにそれぞれ割り当てられた前記公開鍵により暗号化して、各ルータに送信する手順と、

を実行させるためのプログラム。

【0117】

【発明の効果】

本発明によると、構内ネットワーク・システム間で通信されるデータの秘匿を各端末のユーザが特に意識しなくても、暗号化の必要なデータは暗号化されて送信され、受信側において復号化されて配信される。これにより、構内ネットワーク・システム間で通信されるデータを秘匿することができる。

【0118】

また、本発明によると、構内ネットワーク・システム間で通信されるデータの秘匿に必要な情報（共通鍵、公開鍵、秘密鍵等）を中央管理装置によって一元管理することができる。これにより、各ユーザ、ルータ等で個別に秘匿情報を管理することが不要となり、また、通信ネットワーク・システムの変更に対して柔軟に対処することができる。

【図面の簡単な説明】

【図1】

本発明の実施の形態による暗号通信ネットワーク・システムの全体構成を示すブロック図である。

【図 2】

管理データベースが有するデータ（秘匿端末テーブル）を示す。

【図 3】

管理データベースが有するデータ（公開鍵／共通鍵テーブル）を示す。

【図 4】

管理データベースが有するデータ（共通鍵テーブル）を示す。

【図 5】

各ルータが有するデータを示し、（A）は秘匿端末テーブルを、（B）は公開鍵／秘密鍵テーブルを、（C）は共通鍵テーブルを、それぞれ示す。

【図 6】

送信元ルータの処理の流れを示すフローチャートである。

【図 7】

送信先ルータの処理の流れを示すフローチャートである。

【図 8】

管理データベースの秘匿対象テーブル、公開鍵／秘密鍵テーブル、または共通鍵テーブルが更新された場合における中央管理装置の処理の流れを示すフローチャートである。

【図 9】

更新されたテーブルが中央管理装置から送信された場合における送信先ルータの処理の流れを示すフローチャートである。

【符号の説明】

1 0 通信ネットワーク・システム（プライベート・ネットワーク・システム）

1 専用線ネットワーク

2 中央管理装置

3₁～3_n 構内ネットワーク・システム

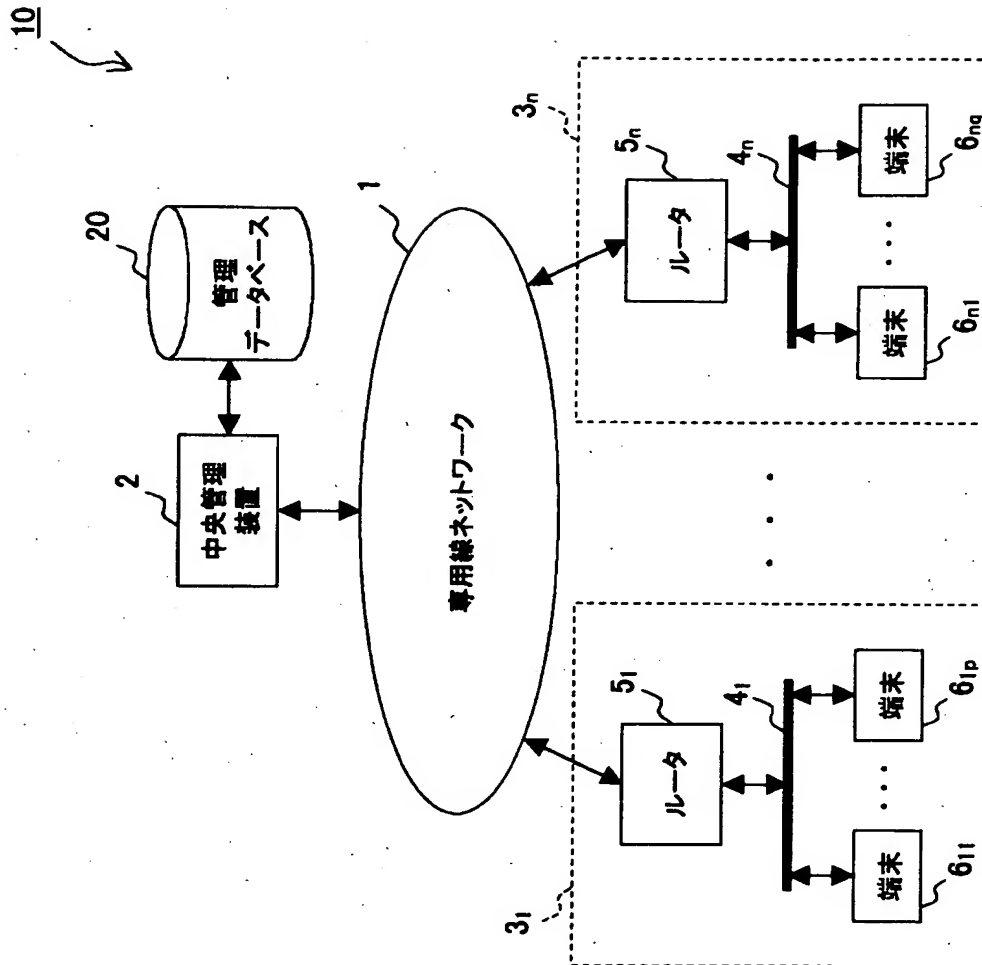
4₁～4_n 構内ネットワーク

$5_1 \sim 5_n$ ルータ

$6_{11} \sim 6_{1p}, 6_{n1} \sim 6_{nq}$ 端末

【書類名】 図面

【図 1】



【図 2】

秘匿端末テーブル

ルータ	加入端末	相手先端末
ルータ5 ₁	端末6 ₁₁	端末6 ₂₁
	端末6 ₁₁	端末6 ₂₅
	⋮	⋮
	端末6 ₁₂	端末6 ₃₂
	端末6 ₁₂	端末6 ₄₄
	⋮	⋮
	端末6 _{1p}	端末6 ₂₂
	⋮	⋮
ルータ5 ₂	⋮	⋮
⋮	⋮	⋮
ルータ5 _n	⋮	⋮

【図 3】

(A) 公開鍵／秘密鍵テーブル

ルータ	公開鍵	秘密鍵
中央管理装置	K _{pc}	K _{sc}
ルータ5 ₁	K _{p1}	K _{s1}
ルータ5 ₂	K _{p2}	K _{s2}
⋮	⋮	⋮
ルータ5 _n	K _{pn}	K _{sn}

(B) 公開鍵／秘密鍵テーブル

ルータ	相手ルータ	公開鍵	秘密鍵
中央管理装置	ルータ5 ₁	K _{pc1}	K _{sc1}
	ルータ5 ₂	K _{pc2}	K _{sc2}
	⋮	⋮	⋮
	ルータ5 _n	K _{pcn}	K _{scn}
ルータ5 ₁	中央管理装置	K _{p1c}	K _{s1c}
	ルータ5 ₂	K _{p12}	K _{s12}
	⋮	⋮	⋮
	ルータ5 _n	K _{p1n}	K _{s1n}
⋮	⋮	⋮	⋮

【図 4】

(A) 共通鍵テーブル

共通鍵
Kc1
Kc2
⋮

(B) 共通鍵テーブル

共通鍵	暗号方法
Kc1	M1
Kc2	M2
⋮	⋮

【図 5】

(A) 秘匿端末テーブル

加入端末	相手先端末
端末6 ₁₁	端末6 ₂₁
端末6 ₁₁	端末6 ₂₅
⋮	⋮
端末6 ₁₂	端末6 ₃₂
端末6 ₁₂	端末6 ₄₄
⋮	⋮
端末6 _{1p}	端末6 ₂₂
⋮	⋮

(B) 公開鍵／秘密鍵テーブル

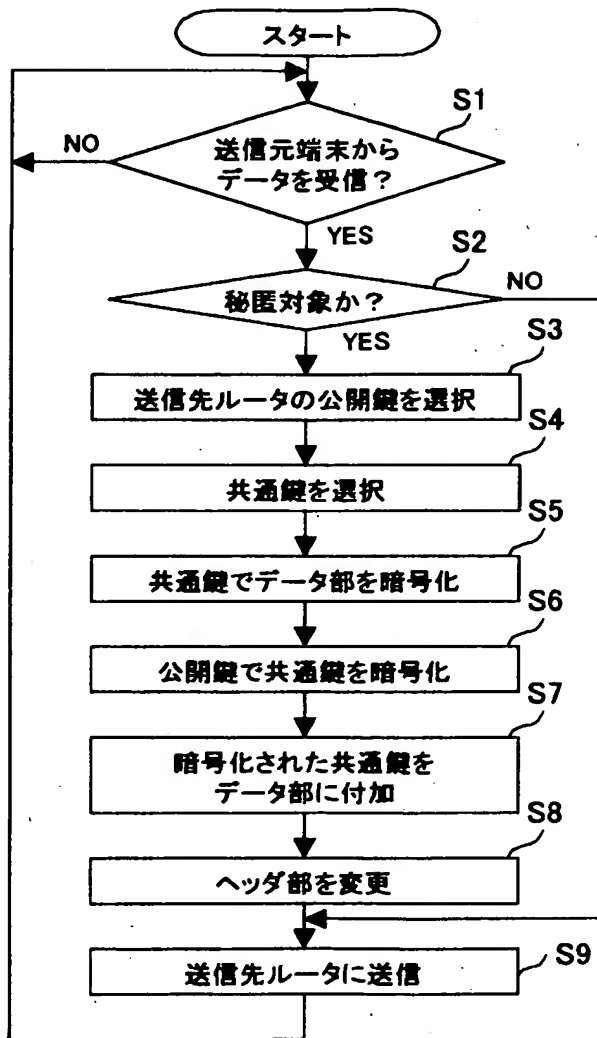
ルータ	公開鍵	秘密鍵
ルータ5 ₁	Kp1	Ks1
ルータ5 ₂	Kp2	
⋮	⋮	⋮
ルータ5 _n	Kpn	
中央管理装置	Kpc	

(C) 共通鍵テーブル

共通鍵
Kc1
Kc2
⋮

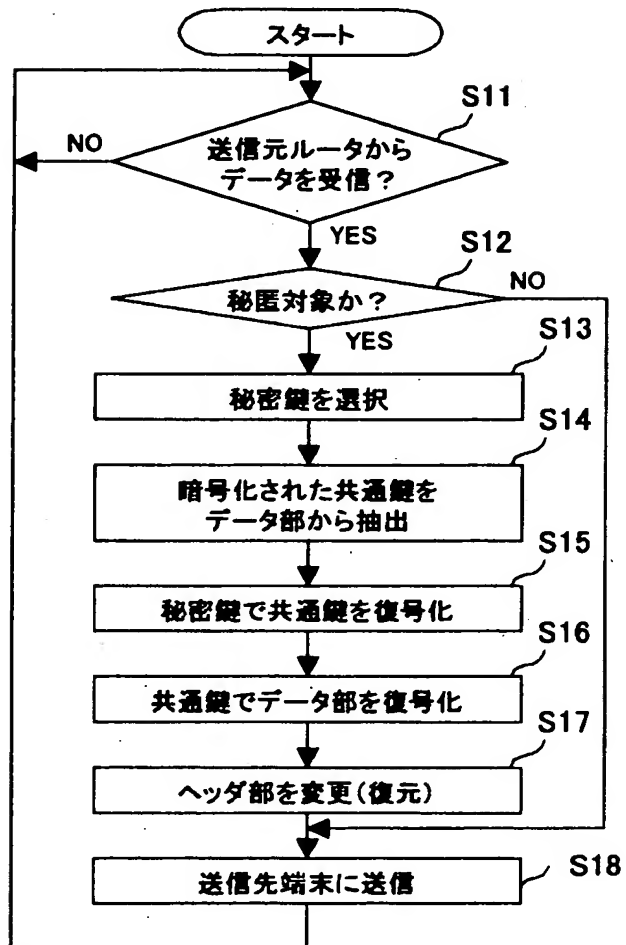
【図 6】

送信元ルータの処理



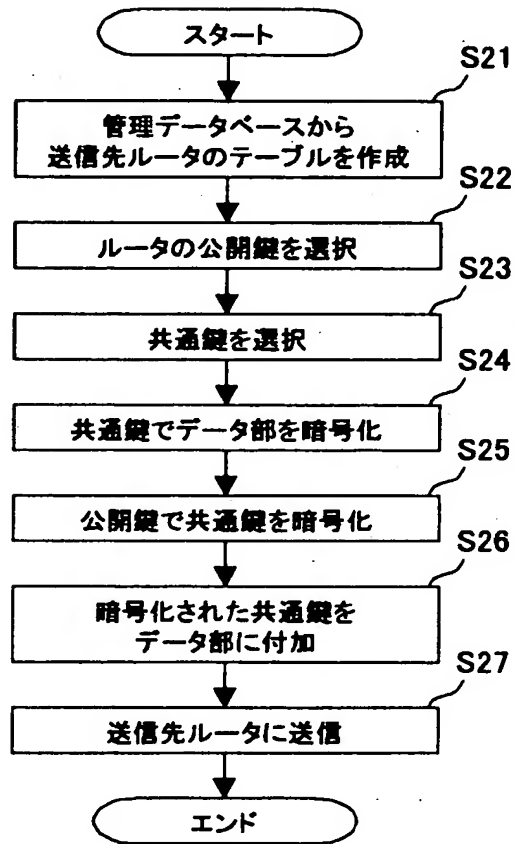
【図 7】

送信先ルータの処理



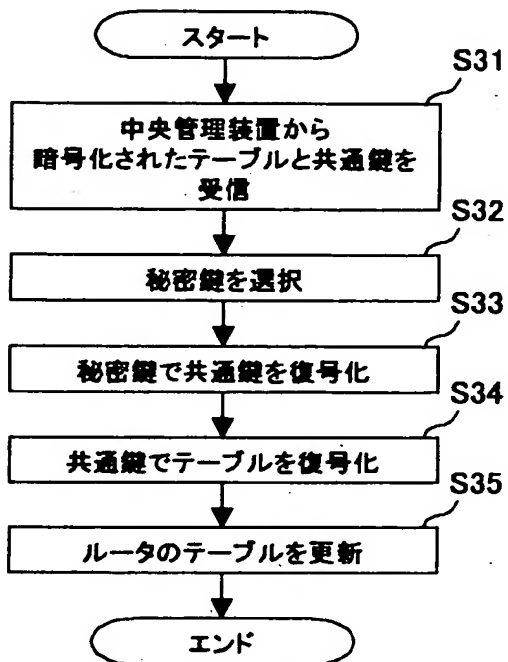
【図 8】

テーブルの更新処理(中央管理装置)



【図 9】

テーブルの更新処理(ルータ側)



【書類名】 要約書

【要約】

【課題】 複数の構内ネットワーク・システムが相互節則された通信ネットワーク・システムにおいて、構内ネットワーク間で通信されるデータの秘匿を図る。

【解決手段】 通信ネットワーク・システム 10 では、中央管理装置 2 と複数の構内ネットワーク・システム 3 とが相互接続され、各構内ネットワーク・システム 3 では、ルータ 5 と端末 6 とが接続されている。中央管理データベース 20 は、共通鍵と、各ルータ 5 および該中央管理装置 2 にそれぞれ割り当てられた公開鍵とを記憶する。中央管理装置 2 は、共通鍵を各ルータ 5 の公開鍵により暗号化して送信する。ルータ 5 は、暗号化された共通鍵を自己の秘密鍵により復号化し、復号化された共通鍵を記憶する。各ルータ 5 は、自己の構内ネットワーク・システム 3 に設けられた送信元端末 6 から他の構内ネットワーク・システム 3 に設けられた送信先端末 6 へ送信される通信データ共通鍵により暗号化して送信する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願2001-288076
受付番号	50101392817
書類名	特許願
担当官	金井 邦仁 3072
作成日	平成13年10月 2日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000005223
【住所又は居所】	神奈川県川崎市中原区上小田中4丁目1番1号
【氏名又は名称】	富士通株式会社

【代理人】

申請人

【識別番号】	100094514
【住所又は居所】	神奈川県横浜市港北区新横浜3-9-5 第三東 昇ビル3階 林・土井 国際特許事務所
【氏名又は名称】	林 恒徳

【代理人】

【識別番号】	100094525
【住所又は居所】	神奈川県横浜市港北区新横浜3-9-5 第三東 昇ビル3階 林・土井 国際特許事務所
【氏名又は名称】	土井 健二

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社